

**LISTING OF THE CLAIMS PER 37 C.F.R. §1.121**

1-241. (Cancelled)

242. (New) A method of redirecting data items from a messaging host system to a user's mobile device, the method comprising the acts of:

establishing a secure communications link between a redirector host system and the user's mobile device;

generating an encryption key at the redirector host system;

storing the encryption key at the redirector host system;

generating a decryption key at the redirector host system;

forwarding the decryption key from the redirector host system to the user's mobile device using the secure communications link;

terminating the secure communications link between the redirector host system and the user's mobile device;

detecting new data items for the user as they arrive at the messaging host system by the redirector host system;

encrypting each new data item to form an encrypted new data item using a cipher algorithm and the encryption key at the redirector host system; and

transmitting the encrypted new data items to the user's mobile device in real-time.

243. (New) The method as recited in claim 242, wherein the act of establishing a secure communications link between a redirector host system and the user's mobile device further comprises establishing a serial connection between the redirector host system and the user's mobile device.

244. (New) The method as recited in claim 242, wherein the act of establishing a secure communications link between a redirector host system and the user's mobile device further comprises using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

245. (New) The method as recited in claim 242, wherein the acts of generating an encryption key at the redirector host system and generating a decryption key at the redirector host system further comprise generating a shared key.

246. (New) The method as recited in claim 242, wherein the encryption key and the decryption key are generated according to a symmetric key encryption scheme.

247. (New) The method as recited in claim 242, wherein the act of generating an encryption key at the redirector host system further comprises generating a public key.

248. (New) The method as recited in claim 247, wherein the act of generating a decryption key at the redirector host system further comprises generating a private key.

249. (New) A system for redirecting data items from a messaging host system to a user's mobile device, the system comprising:

means for facilitating a secure communications link between a redirector host system and the user's mobile device;

means for generating an encryption key at the redirector host system;

means for storing the encryption key at the redirector host system;

means for generating a decryption key at the redirector host system;

means for forwarding the first decryption key from the redirector host system to the user's mobile device using the secure communications link;

means for facilitating termination of the secure communications link between the redirector host system and the user's mobile device;

means for detecting new data items for the user as they arrive at the messaging host system;

means for encrypting each new data item to form an encrypted new data item using a cipher algorithm and the encryption key at the redirector host system; and

means for transmitting the encrypted new data items to the user's mobile device in real-time.

250. (New) The system as recited in claim 249, wherein the means for facilitating a secure communications link between a redirector host system and the user's mobile device further comprises a serial connection between the redirector host system and the user's mobile device.

251. (New) The system as recited in claim 249, wherein the means for facilitating a secure communications link between a redirector host system and the user's mobile device further comprises means for using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

252. (New) The system as recited in claim 249, wherein the means for generating an encryption key at the redirector host system and the means for generating a decryption key at the redirector host system further comprise means for generating a shared key.

253. (New) The system as recited in claim 249, wherein the means for generating an encryption key at the redirector host system and the means for generating a decryption key at the redirector host system further comprise means for generating the encryption key and the decryption key according to a symmetric key encryption scheme.

254. (New) The system as recited in claim 249, wherein the means for generating an encryption key at the redirector host system further comprises means for generating a public key.

255. (New) The system as recited in claim 254, wherein the means for generating a decryption key at the redirector host system further comprises means for generating a private key.

256. (New) A computer-accessible medium having a sequence of instructions which, when executed by a processing entity, effectuate redirection of data items from a messaging host system to a user's mobile device, the computer-accessible medium comprising:

instructions for facilitating a secure communications link between a redirector host system and the user's mobile device;

instructions for generating an encryption key at the redirector host system;

instructions for storing the encryption key at the redirector host system;

instructions for generating a decryption key at the redirector host system;

instructions for forwarding the first decryption key from the redirector host system to the user's mobile device using the secure communications link;

instructions for facilitating termination of the secure communications link between the redirector host system and the user's mobile device;

instructions for detecting new data items for the user as they arrive at the messaging host system;

instructions for encrypting each new data item to form an encrypted new data item using a cipher algorithm and the encryption key at the redirector host system; and

instructions for transmitting the encrypted new data items to the user's mobile device in real-time.

257. (New) The computer-accessible medium as recited in claim 256, wherein the instructions for facilitating a secure communications link between a redirector host system and the user's mobile device further comprises instructions for facilitating a serial connection between the redirector host system and the user's mobile device.



258. (New) The computer-accessible medium as recited in claim 256, wherein the instructions for facilitating a secure communications link between a redirector host system and the user's mobile device further comprises instructions for using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

259. (New) The computer-accessible medium as recited in claim 256, wherein the instructions for generating an encryption key at the redirector host system and generating a decryption key at the redirector host system further comprise instructions for generating a shared key.

260. (New) The computer-accessible medium as recited in claim 256, wherein the instructions for generating an encryption key at the redirector host system and generating a decryption key at the redirector host system further comprise instructions for generating the encryption key and the decryption key according to a symmetric key encryption scheme.

261. (New) The computer-accessible medium as recited in claim 256, wherein the instructions for generating an encryption key at the redirector host system further comprises instructions for generating a public key.

262. (New) The computer-accessible medium as recited in claim 256, wherein the instructions for generating a decryption key at the redirector host system further comprises instructions for generating a private key.